Theme article : The Internet of Things : The Big Picture

Prof. Dileeka Dias

1.What is the Internet of Things?

The term Internet of Things (IoT) generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single, universal definition.

The Internet of Things term was coined by Kevin Ashton executive director of the Auto-ID Center in 1999, in the context of supply chain management. Around the same time, Neil Gershenfeld was speaking about similar things from the MIT Media Lab in his book When Things Start to Think.

The IoT extends the Internet and

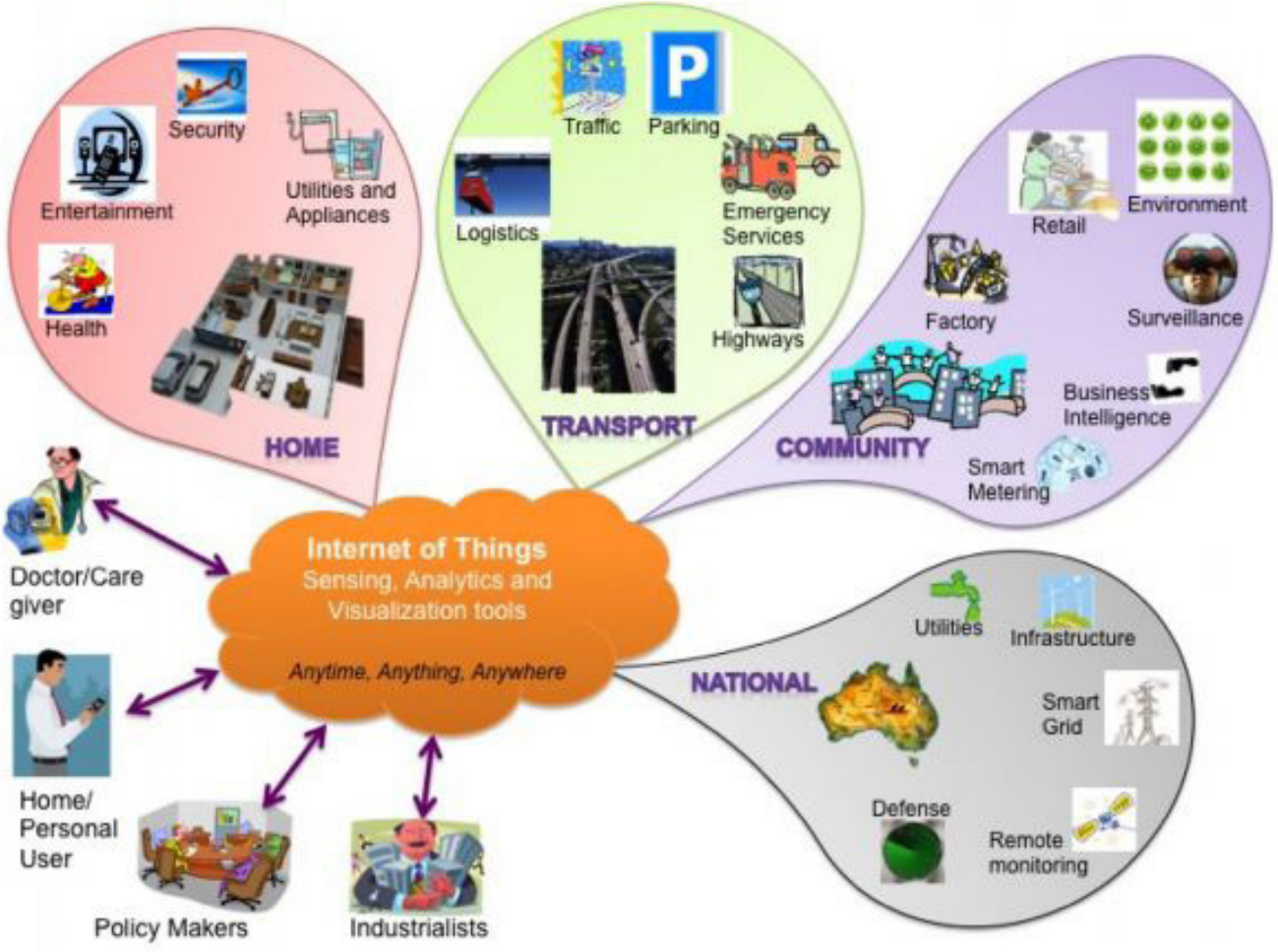

Fig. 1 : Possible application areas of IoT

the Web to the physical world, through the deployment of devices with embedded identification, sensing and/or actuation and communication capabilities. The devices are linked through information and communication technologies based on the Internet Protocol (IP), and will enable Internet connectivity for everyday objects in homes, roads and vehicles, utilities, factories, battlefields, the environment, and even on our bodies. Such objects are generally referred to as smart objects, and the applications they make possible smart scenarios.

The IoT thus builds on three pillars, related to the ability of smart objects to: (i) be identifiable (anything identifies itself), (ii) to communicate (anything communicates) and (iii) to interact (anything interacts) – either among themselves, building networks of interconnected objects, or with end-users or other entities in the network. It is a complex concept that cuts across multiple disciplines, and that depends on synergetic efforts from several communities such as telecommunication industry, device manufacturers, semantic Web, and informatics for its success. The IoT offers a platform for everyone from garage hobbyists to technology giants to innovate.

Combined with powerful data analytic capabilities, the IoT is envisioned to enable entirely new areas of applications and services having great technical, social, economic and political significance. It promises to transform the way people work, live and play, and the way governments make policies and decisions. Projections for the impact of IoT on the Internet and the economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025. Figure 1 illustrates some possible application areas.

This article provides an overview of the Internet of Things. To make it easier for the reader to understand the IoT paradigm, we initially illustrate some IoT applications being implemented, proposed or researched. Next we look at IoT systems in detail, in terms of their key components. Finally we present some challenges for the real-life deployment of the IoT and its acceptance by potential users.

Several articles in this issue to follow, will highlight specific aspects of IoT such as applications and devices, communication and networking, and security and privacy.

2.IoT Applications

The IoT enables us to create a self-aware environment where we know exactly what is happening around us. From personal health to home security, from agriculture to urban traffic control, from utility metering to law enhancement, from entertainment to public safety, the

Table 1. Applications identified by the City of Melbourne

Citizens	
Healthcare	Triage, patient monitoring personnel monitoring, disease spread modelling and containment – real- time health status and predictive information to assist practitioners in the field, or policy decision in pandemic scenarios
Emergency services, defense	Remote personnel monitoring (health, location); resource management and distribution, response planning; sensors built into building infrastructure to guide first responders in emergencies or disaster scenarios
Crowd monitoring	Crowd flow monitoring for emergency management, efficient use of public and retail spaces; workflow in commercial environment
Transport	
Traffic managementInfrastructure monitoring	Intelligent transportation through real-time traffic information and path optimization Sensors built in to infrastructure to monitor structural fatigue and other maintenance; accident monitoring for incident management and emergency response coordination
Services	
Water	Water quality, leakage, usage, distribution, waste management
Building management	Temperature, humidity control, activity monitoring for energy usage management,
Environment	D heating, Ventilation and air conditioning (HVAC), Air pollution, noise monitoring, waterways, industry monitoring

Fig. 2 : Elements of an IoT system

applications proposed for IoT are too many to discuss in detail. In this Section we highlight only a few. One of many possible ways of classifying IoT applications is as shown in Figure 1. The Home domain utilizes IoT at the personal level, and the Transport and Community domains at the enterprise level. Application examples in the National domain include infrastructure, defense, utilities and public services. Whatever classification we adopt for IoT applications, there is a significant overlap in applications and the use of data between domains. The Internet and widespread mobile connectivity enable sharing of data between different applications in a seamless manner creating multiple business opportunities. For instance, Home IoT produces electricity usage data in the house and makes it available to the electricity (utility) company, which can in turn optimize the supply and demand with its national level utility IoT applications.

2.1.Personal and Home IoT

A number of possible IoT application concepts and their benefits are listed below. A number of electronic manufacturers as well as all mobile device platforms offer applications of this nature supported by mobile data communication technologies. However, a common platform and standards for this type of services is yet to emerge.

• Healthcare in the home, utilizes body area sensors measuring physiological parameters and smartphones to collect heath information at an IoT back-end, through which a variety of ubiquitous healthcare services can be provided.

• Care of the elderly in their homes which may use IoT for monitoring people in their home environments, providing early intervention and treatment.

• Control of home equipment such as lights, air conditioners, refrigerators etc. to better manage home energy utilization.

• Home security is an area where we find a growing range of IoT application, integrating a variety of sensing mechanisms for intrusion detection.

• Individual devices ('things') in the home can periodically send notifications via social media such as Facebook and Twitter. This is envisaged to be a transformation of social networking due to the IoT.

2.2.Enterprise IoT

Enterprise IoT applications can be broadly termed Smart Environments, which may include buildings, infrastructure,

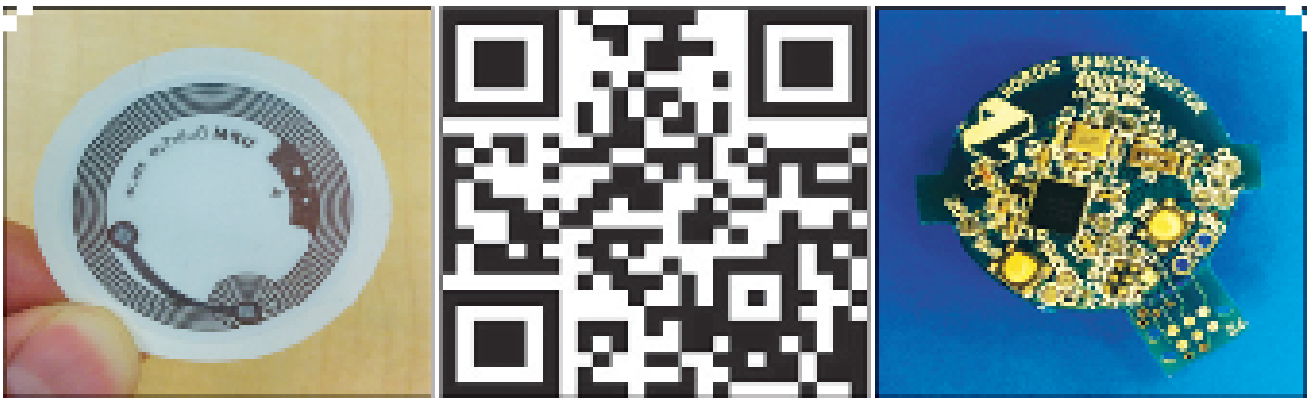

Fig. 3 : Tagging technologies for identification of IoT devices. (a) NFC, (b) QR code, (c) BLE tag

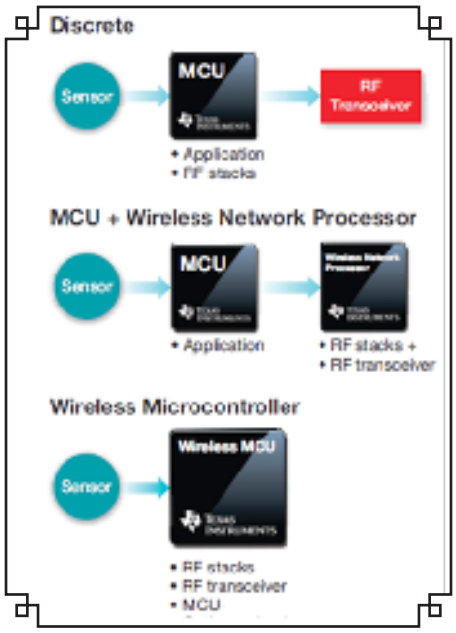

Fig. 4 : IoT device electronics

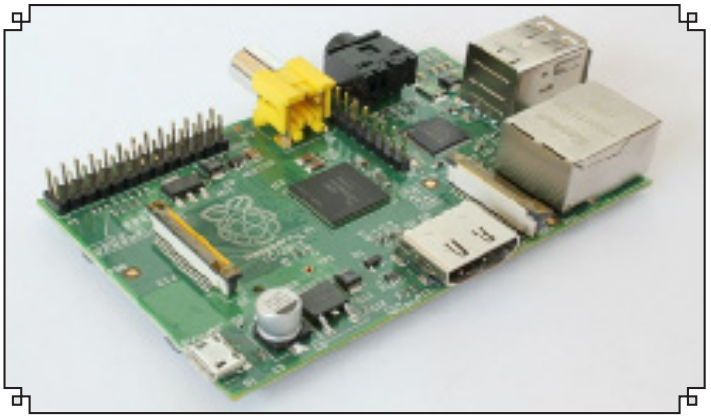

Fig. 5 : The Raspberry Pi, a credit - card sized single board computer

traffic, utilities, and the general environment. As examples, some applications identified by the City of Melbourne are listed in Table 1 below. These applications are grouped according to their impact areas: citizens (health and wellbeing), transport (mobility, productivity, pollution), and critical community services managed and provided by the local government to city inhabitants. Here too, applications share data among them for mutual benefit.

2.3.Utility IoT

Utility IoT applications target service optimization, i.e., for resource management in order to optimize cost vs. profit. These applications are envisaged to be made up of very extensive networks operated by large organizations on a regional or national scale. Applications involving electricity and water supply management are of high priority in the utility IoT arena.

Smart grid and smart metering are key utility IoT applications being rolled out around the world currently. The benefits of these applications are two-fold. First, they help consumers to achieve energy efficiency by modifying their electricity consumption patterns. Secondly, they help the electricity companies to maintain the load balance within the grid, ensuring high quality of service .

Water network monitoring is another valuable IoT service. Sensors measuring critical water quality parameters installed at key locations will be able to ensure the quality assurance of drinking water. This may avoid or provide early warning of contamination of water supplies. Along similar lines, agriculture-related monitoring applications are growing in pilot level IoT implementations. Among the functions offered by these include soil moisture monitoring, automatic watering and fertilization.

3.Elements and Enablers of IoT

The six main building blocks

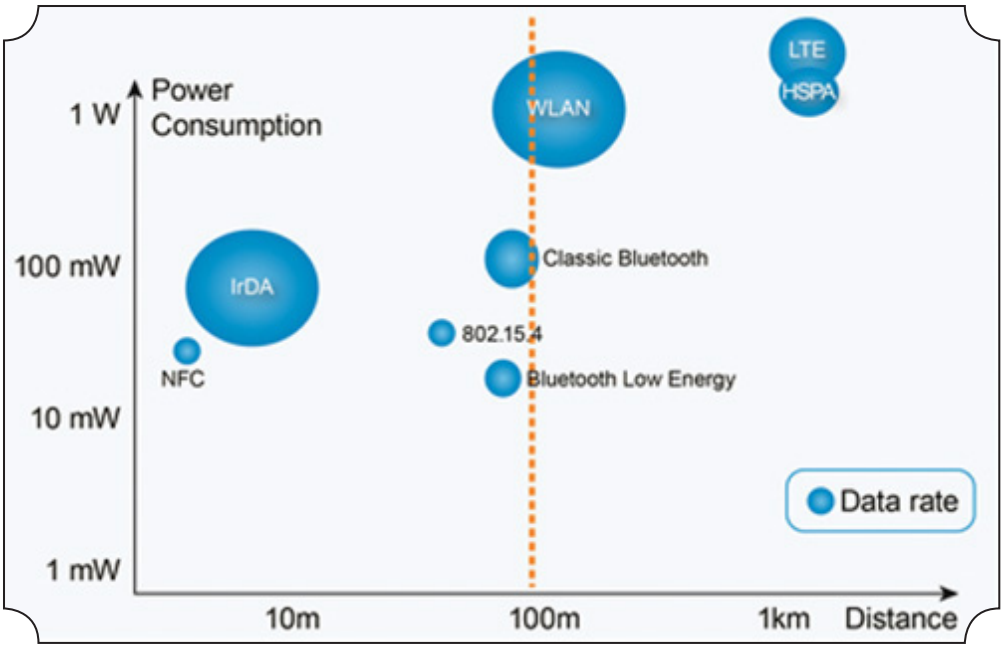

Fig. 6 : Comparison of power consumption, range and data rate of short-range communication technologies

	Bluetooth Low Energy	802.15.4	WLAN
Cost	✓	✓(✓)	✓
Security	✓	✓	✓
Power consumption	✓	✓	×
Ecosystem	✓	×	✓
Reliability	✓	✓	✓
Ease of use	✓	✓	✓
Range	✓	✓(✓)	✓

	Bluetooth Low Energy	802.15.4	WLAN	NFC
Remote control	✓	✓	✓	×
Security	✓	✓	✓	✓
Health and Fitness	✓	✓	✓	×
Home and Building	✓	✓	✓	×
Industrial	✓	✓	✓	×
Positioning	✓	✓	✓	×
Payment	✓	×	×	✓
Automotive	✓	×	✓	✓
Comments	Largest ecosystem (phones, tablets, ...). Low power.	Low power but closed ecosystem. Established in some use cases e.g. Smart Energy	Large ecosystem but higher power. Infrastructure use.	Low power but very short range

Fig. 7 : Silent characteristics of short - range communication technologies and their suitability for different applications

needed to deliver the functionality of IoT are illustrated in Figure 2. This section looks at these building blocks in detail, along with examples of available technologies and realizations in each case.

3.1. Identification

Identification is essential in the IoT to name and match services with their demand. Electronic Product Codes (EPCs) is an example of a universal identifier that gives a unique identity to a specific physical object that it is attached to. EPCs are encoded on Radio Frequency Identification (RFID) tags which can be used to track all kinds of objects including trade items, fixed assets, documents, or reusable transport items. A reader would transmit a query signal to the tag and receive the reflected signal containing the EPC. RFID tags can be passive, active or semi-passive. Passive tags are very cheap, but depend solely on the electromagnetic energy supplied by the reader. Active tags self-powered, and thus have a longer reading range, but is higher in cost than a passive tag.

RFID was considered one of the most likely technologies to accelerate the formation of the IoT. Though RFID has become very popular in logistics applications, it has not been successful in the wider arena of IoT for identification, perhaps the major reason being the absence of support for it in mobile phones, thus needing a special reader. A more advanced and secure form of RFID, Near Field Communication (NFC) is strongly promoted for applications involving electronic payments. Smartphone manufacturers are now integrating NFC into their devices, adding to the potential of this technology as a key enabler for IoT.

Another contender for low-cost tagging is the optical or printed tag. The most popular is the Quick Response (QR) code. The QR code can be read by an ubiquitous mobile application and a camera found in all modern smartphones. QR codes are widely used on many products, newspapers an advertising material.

A promising new technology in the device tagging space is Bluetooth low energy (BLE). All smartphones released in the last few years have BLE built in. With BLE, small low cost electronic tags can be implemented, which can signal their presence wirelessly.

Figure 3 shows the three tagging technologies discussed above.

An object's identity may not be

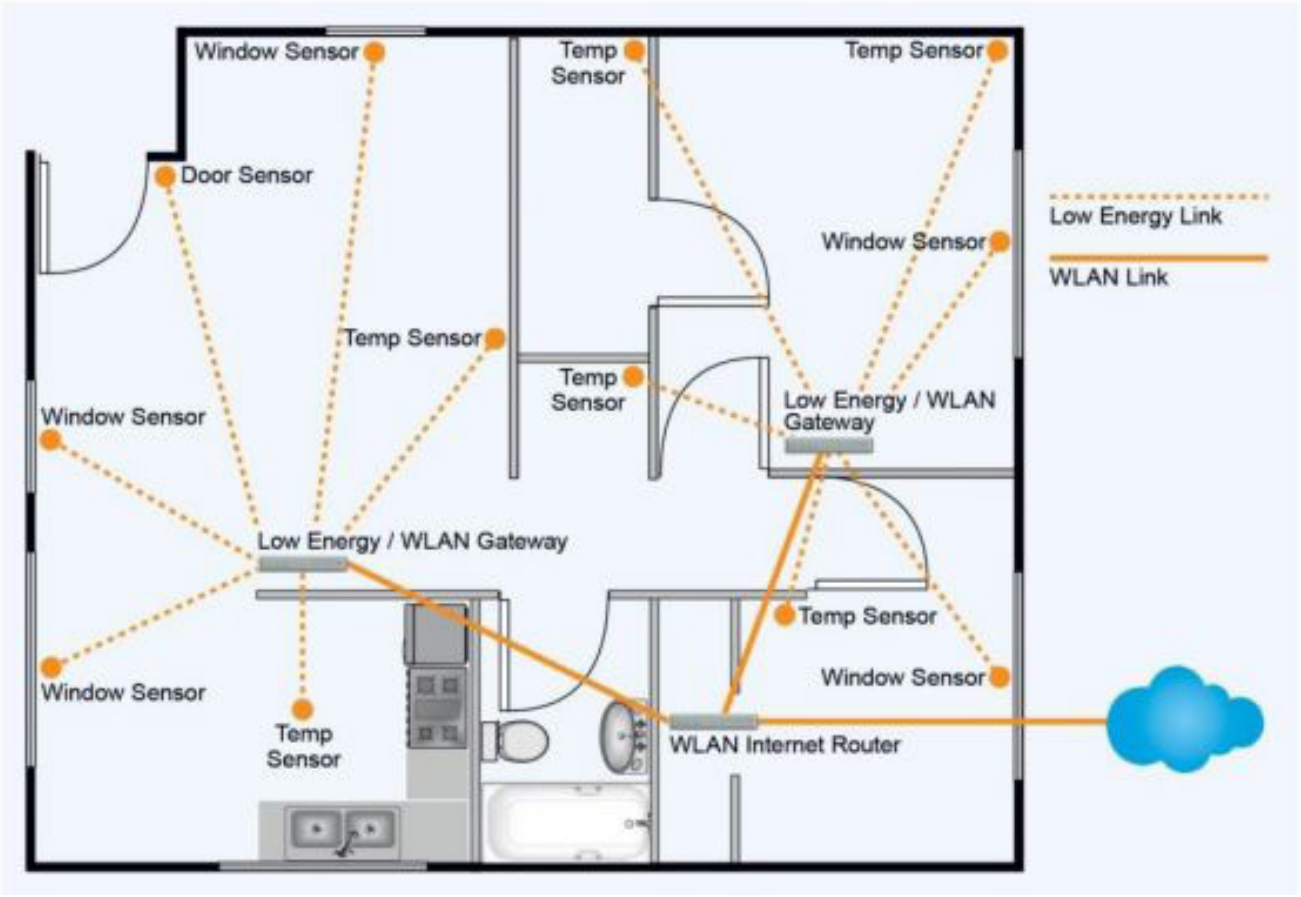

Fig. 8 : Networking architecture for IoT in a typical Smart Home application supporting several communication technologies

always globally unique. In such an event unique address is needed to identify objects within the communications network. IPv6 has been proposed as an addressing scheme for IoT objects, due to the very large number of objects expected to be connected in future.

3.2.Sensing

Sensing in the IoT is done by smart sensors and actuators. IoT devices are of different levels of integration, and contains sensing elements, actuator elements, data processing and control subsystems (a microcontroller) and a wireless communication mechanism (an RF transceiver). The devices are programmable, allowing the designer the flexibility to build in the functions required of the device. Figure 4 shows different levels of integration available in popular electronic devices. In the Discrete option, the microcontroller and the RF transceiver are two separate devices. The Wireless Microcontroller on the other hand is capable of interfacing to the sensor, data processing and control functions as well as wireless communications. At a more sophisticated level, IoT devices may be built around single board computers (SBCs) integrated with single-board computers and built-in security and communications protocols. The Raspberry Pi shown in Figure 5, is an increasingly popular SBC among IoT enthusiasts. Many other hardware platforms too have become available to implement IoT devices such as Arduino, Friendly ARM, Intel Galileo, Gadgeteer, BeagleBone, WiSense, T-Mote Sky etc. Though the high cost of such devices prevent them from being used extensively, they are suitable for special purpose applications and lend to quick prototyping and application development due to the availability of a wide variety of developer tools and standard interfaces. However, expert electronics designers will be able to develop their own devices from scratch, better optimizing cost, power and other resources specific to their application.

RFID, originally intended for simple, passive identification of objects has been proposed as a generic sensing platform for IoT applications in healthcare. This technology promises low cost, reconfigurable, disposable sensors

Table 2. IoT Services

Service Class	Description	Examples
Identity-related services	These are the most basic type, and are used in other types of services.	Every application that needs to use real world objects has to identify these objects.
Information aggregation services	These collect and summarize raw data that need to be processed and reported to the IoT application.	• Smart healthcare systems embed sensors and actuators in patients' and their medicine for monitoring and tracking purposes. Clinical care personnel monitor physiological statuses of patients through data collected, analyze them and forward to relevant persons for action.
Collaborative aware services	These act on top of Information aggregation services and use the obtained data to make decisions and react accordingly.	• Smart grids use the IoT to connect millions of electricity meters to the network of energy providers. These meters collect, analyze and control energy consumption, reduces potential failures and increase efficiency • A smart home can automatically close windows based on the weather forecast. • A smart building system can detect when an appliance is faulty and send maintenance requests automatically. • Self-driving cars are future examples of future ITS. • Industrial automation systems work by allowing groups of machines to produce products quickly and more accurately. IoT is utlized to monitor and control production line functions.
Ubiquitous services	These aim to provide Collaborative-aware services anytime, to anyone, and anywhere.	The ultimate goal of all IoT applications is to reach the level of ubiquitous services. However, there are many remaining challenges that have to be addressed. • A smart city can be seen as an application of ubiquitous services. This aims to improve the quality of life in the city in a variety of ways. Various systems employing smart technologies are interconnected to provide required services (health, utilities, transportation, government, buildings and homes)

for future IoT systems.
IoT devices currently available, and the applications they make possible will be further illustrated in a later article in this issue.

3.3.Communication

The IoT communication technologies connect different types of devices together and/or to a central facility to deliver specific services. The important communications requirements for IoT include energy efficient operation , reliability and scalability.

Fig. 9 : The "Knowledge hierarchy" in the context of IoT

Depending on the application, factors such as range, data requirements, security and power demands and battery life will dictate the choice of one or some form of combination of technologies. There is a wide choice of communication options for engineers and application developers working on products and systems for the Internet of Things (IoT). Many technologies are well known, such as WiFi, Bluetooth, ZigBee (IEEE802.15.4) and 2G/3G/4G cellular. There are also several new emerging networking options such as Thread as an alternative for home automation applications, and low-power, long-range technologies such as LoRa.
In this article we look at three technologies WiFi (WLAN), Bluetooth, including Bluetooth Low Energy (BLE) and IEEE802.15.4 as options for low-power, short-range communications for IoT devices. Further information will be available in a later article in this issue.

Figure 6 compares the three most important features, power consumption, data rate and communication range of the above technologies. These provide connectivity in the "Last 100 Meters" of an IoT network.
It is clearly evident that each technology has its unique strengths and weaknesses. WiFi has the advantages of being available in mobile devices (the availability of an 'ecosystem') and high data rate, while the key disadvantage is high power consumption. BLE on the other hand is able to support lower data rates, but with significantly less power consumption. Zigbee (802.15.4) is similar in these characteristics to BLE, but has the added advantage of being able to extend network range by working in a mesh configuration. The salient characteristics of each technology and the type of applications they are most suited for are highlighted in Figure 7.

In order to enable a variety of devices with different communication technologies to communicate in an integrated manner, the evolving networking architecture for IoT is illustrated in Figure 8 for a typical Smart Home scenario. The home has an Internet router from a service provider, which provides WiFi access to devices within the home. However, WiFi is not a suitable option for IoT devices, due to its high power consumption. Therefore, the home is equipped with two miniature gateways, each communicating via BLE in the downstream with the IoT devices, and via WiFi in the upstream with the Internet router. Through this network configuration, the IoT devices are able to send/receive data to the Internet, to be used in suitable Smart Home applications. Gateways having technologies such as BLE, Zigbee and Z-wave in the downstream and WiFi in the upstream are becoming available, along with a multitude of IoT sensors/actuators.

3.4.Computation

Computation in the IoT may take place either in the devices or centrally in the cloud, or both. In the devices, computation is supported in hardware by the internal processor units (microprocessors, microcontrollers, FPGAs etc.) and memory and in software by operating systems where available. The cloud provides facilities to process big data collected from a large number of devices in real-time, and extract knowledge that is useful for all users. Thus, the Computation component powers the "brain" of the IoT system, the "brain" itself being the Semantics component to be described later.

There are several Real-Time Operating Systems (RTOS) that are suitable for IoT applications. Contiki and TinyOS are such

operating systems that have been widely used in wireless sensors, even before the arrival of the IoT paradigm. These are lightweight operating systems suitable for resource constrained (enbattery life, memory, processing power) IoT environments. Google, along with a consortium of automobile manufacturers has recently released Android Auto, to allow mobile devices running the Android operating system to be operated in automobile dashboards, to accelerate the adoption of the Internet of Vehicles (IoV) paradigm.

Cloud platforms form the other important computational part of the IoT. Connecting a large number of physical objects equipped with sensors to the Internet generates what is called "big data". Big data needs smart and efficient storage. Due to its large volume, big data needs special hardware environments and software tools to capture, manage and process them within an acceptable time. Cloud services allow users to access remote facilities to do these, and extract knowledge by complex processing of data captured through the IoT. Therefore, cloud computing presents a good choice for IoT's computational requirements.

There are many free and commercial cloud platforms and frameworks available to host IoT services such as ThingWorx, OpenIoT, Google Cloud, Amazon, GENI etc.

3.5.Services

IoT services are made available to applications. Services can be categorized under four classes, and are summarized in Table 2.

3.6.Semantics

A primary goal of interconnecting devices and collecting/processing data from them is to create situation awareness and enable applications, machines and human users to better understand their surroundings. Data collected by devices is usually multimodal (temperature, light, sound, video etc.) and diverse in nature (e.g. quality of data can vary). These make the task of processing, integrating and interpreting real world data a challenging task. This data transformation process may be illustrated using the "knowledge hierarchy" as in Figure 9.

To exploit the full potential of the IoT, we need to transform raw data into actionable intelligence (wisdom).

While "big data" solutions and cloud platforms can provide infrastructure and tools for handling and analyzing huge volumes of IoT data, we still need efficient methods and solutions that can structure, annotate, share and make sense of the IoT data and facilitate turning it into actionable knowledge in different application domains. These issues naturally lead to a semantic-oriented perspective

Table 3. Technologies for the IoT

IoT Elements		Samples
Identification	Naming	EPC, uCode
	Addressing	IPv4, IPv6
Sensing		Smart Sensors, Wearable sensing devices, Embedded sensors, Actuators, RFID tag
Communication		RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, WiFi, WiFiDirect, , LTE-A
Computation	Hardware	SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubieboard, Smart Phones
	Software	OS (Contiki, TinyOS, LiteOS, Riot OS, Android); Cloud (Nimbits, Hadoop, etc.)
Service		Identity-related (shipping), Information Aggregation (smart grid), Collaborative-Aware (smart home), Ubiquitous (smart city)
Semantic		RDF, OWL, EXI

towards the IoT.
The suite of technologies developed in the Semantic Web, such as Linked Data, the Resource Description Framework (RDF) and the Web Ontology Language (OWL) and semantic web services, can be used as principal solutions for IoT. Thus, semantics represents the "brain" of the IoT.
In this section, we have reviewed the main component building block of the IoT, , along with examples of available technologies and realizations in each case. Table 3 summarizes these technologies in each component.

4.Challenges of IoT

Despite the potential, positive predictions, and the glamour surrounding the Internet of Things, there are significant challenges that could stand in the way of realizing its potential benefits. Some key challenges are presented below.

4.1.Security and Privacy

The most serious of IoT challenges are security and privacy. The Physical Web could enable hackers to control our devices unless precautions are taken. It is unclear if conventional, well-established security measures that exist for the Web are suitable or even adequate for IoT applications.

Social threats can occur when information is inferred in unexpected ways. For example, the energy consumption information of a house would indicate the times at which the house is unoccupied. This information may be used to turn off unnecessary appliances in the house to save energy, and also to break into the house. Thus, it is important that the information obtained via the IoT does not fall into unauthorized hands. Movements can be tracked and activities inferred, though multiple streams of data collected from devices with and around a person without the individual being aware of it. Features of IoT that may provide a benefit to an informed user can pose a privacy problem for those who are unaware of the presence of the devices or have no influence on how the information is collected and used.

4.2.Regulatory and Legal

The IoT also poses a wide range of challenges and questions from a regulatory and legal perspective. In some cases, it may even create new legal and regulatory situations and concerns over civil rights that didn't exist prior to these devices. For instance, data collected by IoT devices on jurisdiction may be stored and/or processed in another jurisdiction. These devices use the Internet to communicate across jurisdictions, often with no technical roadblocks. Ownership and protection of data, some of which may be personal or sensitive is an issue which needs careful consideration.

4.3.Standardization

IoT solutions deliver the most value when they are connected to a web of interlinked services. For instance, a smart home solution can deliver significant value only when it integrates the electrical, safety and surveillance systems. However, IoT solutions available today, are highly proprietary, providing little support for integration of devices and services from third parties. The reason for this is the lack of standards spanning industries, vendors and products. The true potential of the IoT can only be exploited to the fullest only when such standards are available.

5.Summary and Conclusion

The concept of combining computers, sensors, and networks to monitor and control devices has existed for decades. The recent confluence of several technology market trends, however, is bringing the Internet of Things closer to widespread reality. These include Ubiquitous Connectivity, Widespread Adoption of IP-based Networking, Computing Economics, Miniaturization, Advances in Data Analytics, and the Rise of Cloud Computing.
This article attempted to provide an overview of the Internet of Things paradigm, with an emphasis on the above aspects. Elements of an IoT system, applications, and concerns/ challenges were discussed. Subsequent articles in this issue will deal in more detail, with emerging applications, communications, networking and security aspects surrounding the IoT.

Prof. Dileeka Dias
BSc.Eng.(Moratuwa),M.S.(Calif.), Ph.D(Calif), MIE(SL), C.Eng., MIEEE
0777688861